MEMORANDUM FOR: DOUGLAS SMALL
Deputy Assistant Secretary for Employment
and Training

FROM: ELLIOT P. LEWIS
Assistant Inspector General
for Audit

SUBJECT: Status of Recommendations
State of California Workforce Agency
Unemployment Insurance Tax and Benefit
Systems Security Audit
Report No. 23-03-005-03-315

This memorandum transmits the results of the Office of Inspector General's (OIG) resolution follow-up audit work on the recommendations from an audit issued February 27, 2003, to the Employment and Training Administration. Our work was performed to determine the current resolution status of recommendations made in the subject report, and includes corrective actions completed by California Employment Development Department and verified by the OIG as of November 30, 2007.

The resolution status of each recommendation, including an explanation of the corrective actions needed to close any remaining open recommendations, is summarized for you in the attached document. Any recommendations that were previously closed, either in the February 2003 report or an earlier resolution memorandum from OIG, dated March 2005, are not listed in this document.

The February 2003 audit report contained 20 findings and 40 corresponding recommendations, of which 39 were resolved and 1 was unresolved. Our March 2005 resolution memorandum, which updated the recommendation status, reflected that 15 of the 40 recommendations were closed. The remaining 25 recommendations all were resolved. Based on our most recent work, we closed 18 additional recommendations, leaving 7 recommendations that still require action. All of the 7 recommendations are resolved.

We request that ETA perform a follow-up review of the remaining resolved recommendations and notify OIG of the progress to close each recommendation. OIG will evaluate the stated progress and any additional documentation provided by the State of California and/or ETA in determining closure of each recommendation. This information believed to represent the agency's progress in resolving and closing the remaining recommendations should be provided to Tracy Katz, Audit Manager, Office of Information Technology Audits (OITA), at 202-693-5161.

Please contact Keith E. Galayda, Director, OITA, at 202-693-5259, if you have any questions.

Attachment

ATTACHMENT

The table below summarizes the prior and current resolution status of the high- and medium-risk recommendations. We have noted in bold, in the current status column, the recommendations that were most recently changed from resolved to closed, and have highlighted with check marks the 7 recommendations that remain resolved.

Finding	Prior Status of Recommendation as of March 2005	Current Status of Recommendation as of November 2007
High-Risk Security Control Recommendations		
High-Risk #1	R1 – Resolved R2 – Closed	R1 – Resolved R2 – Closed
High-Risk #2	Resolved	Resolved
High-Risk #3	Closed	Closed
High-Risk #4	Resolved	Resolved
High-Risk #5	Resolved	Resolved
High-Risk #6	Resolved	**Closed (1)**
High-Risk #7	R1 – Closed R2 – Resolved	R1 – Closed R2 – **Closed (2)**
High-Risk #8	Closed	Closed
High-Risk #9	Resolved	**Closed (3)**
High-Risk #10	R1 – Resolved R2 – Resolved R3 – Resolved R4 – Resolved	R1 – **Closed (4)** R2 – **Closed (5)** R3 – **Closed (6)** R4 – **Closed (7)**
High-Risk #11	R1 – Closed R2 – Closed R3 – Resolved R4 – Closed R5 – Closed R6 – Resolved R7 – Resolved	R1 – Closed R2 – Closed R3 – **Closed (8)** R4 – Closed R5 – Closed R6 – **Closed (9)** R7 – **Closed (10)**
Medium-Risk Security Control Recommendations		
Medium-Risk #1	Resolved	Resolved
Medium-Risk #2	Resolved	Resolved
Medium-Risk #3	Closed	Closed
Medium-Risk #4	R1 – Closed R2 – Resolved R3 – Resolved	R1 – Closed R2 – Resolved R3 – **Closed (1)**
Medium-Risk #5	Closed	Closed
Medium-Risk #6	Closed	Closed
Medium-Risk #7	Closed	Closed
Medium-Risk #8	R1 – Resolved R2 – Resolved R3 – Resolved R4 – Closed R5 – Resolved	R1 – **Closed (2)** R2 – **Closed (3)** R3 – **Closed (4)** R4 – Closed R5 – **Closed (5)**
Medium-Risk #9	R1 – Resolved R2 – Resolved R3 – Resolved R4 – Closed	R1 – **Closed (6)** R2 – **Closed (7)** R3 – **Closed (8)** R4 – Closed

The 7 recommendations that remain resolved are from four high-risk and three medium-risk findings. Detail for the 7 recommendations that remain resolved follows further below, including the corrective actions needed to close them.

High-Risk (HR) Findings:

HR #1 - Recommendations

The Assistant Secretary for Employment and Training Administration (ETA) should ensure that EDD management takes the following actions:

Perform and document risk assessments of existing systems, applications, and networks maintained by EDD and the HHSDC that consider:

- *The sensitivity and integrity of the data;*
- *Threat sources, natural and manmade;*
- *System vulnerabilities, flaws, or weaknesses;*
- *Whether security requirements in place adequately mitigate vulnerabilities;*
- *Mission/business impact and additional controls identified to mitigate risks; and*
- *Final risk determination with management approval.*

The State of California's Employment Development Department (EDD) has a risk assessment matrix that considers four of the six requirements set forth by the recommendation; however, the risk assessment does not include sensitivity and integrity of data or final risk determination with management approval and is not complete for all existing systems, applications and networks maintained by EDD & HHSDC. Consequently, the recommendation remains **resolved.** To close this recommendation, ETA needs to provide the OIG with the final risk assessments for the existing systems, applications and networks and should make sure that it addresses sensitivity and integrity of data and final risk determination with management approval.

HR #2 - Recommendation

The Assistant Secretary for ETA should ensure that EDD develop and implement System Security Plans (SSPs) for its UI Tax and Benefit systems that includes EDD's existing security policies and additional security requirements.

The comprehensive SSPs should be documented in accordance with the NIST standards and should include a "Rules of Behavior". The SSPs should be approved by management and reviewed and updated periodically to reflect any changes to the current environment and the risks associated with those changes.

EDD provided the OIG an Executive Notice and the Information Security Rules of Behavior.

The Notice gave information about responsibilities of a user with respect to EDD technology, and the Rules of Behavior included a confidentiality statement signature page and established behavior for EDD information users. However, the SSPs are in development and the Rules of Behavior are in draft. This recommendation remains **resolved.** To close this recommendation, ETA needs to provide documentation to the OIG that shows it has created an SSP that follows NIST standards and includes a final Rules of Behavior.

HR #4 - Recommendation
The Assistant Secretary for ETA should ensure that EDD's UI Tax and Benefit systems be certified and accredited, in accordance with the criteria set forth within OMB Circular A-130, Appendix III.

As part of the certification and accreditation process, EDD should complete a risk assessment and develop a system security plan for the UI Tax and Benefit systems. In the interim, system owners should obtain interim accreditation statements, which represent the owners' explicit acceptance of risk for their systems, based on the results of any security reviews or audits.

EDD has developed a draft certification and accreditation policy; however, the certification and accreditation are pending the completion of the Risk Assessment report and the completion of the system security plans. This recommendation remains **resolved.** To close this recommendation, ETA needs to provide the OIG a copy of EDD's certification and accreditation policy and procedures, along with the documents that support the completion of the certification and accreditation of the California UI Tax and Benefit systems.

HR #5 - Recommendation
The Assistant Secretary for ETA should ensure that EDD performs a technical evaluation and an application controls review of the UI Tax and Benefit systems to ensure that security controls in place are operating as designed and are compliant with the technical guidelines set forth by OMB A-130 and NIST SP 800-18.

EDD provided the OIG a California UI Work Plan that addresses the controls to be reviewed, the project's objectives and the work that will be accomplished; however, there has been no identification or evaluation or review of controls. This recommendation remains **resolved.** To close this recommendation, ETA needs to provide documentation that control reviews were completed for the California UI and Tax Benefit systems, that the completed global security review of the UI program has been documented, and the corrective action plan for any identified issues during these security reviews, if applicable.

Medium-Risk (MR) Findings:

MR #1 – Recommendation
The Assistant Secretary for ETA should ensure that EDD's SDLC methodology documents be approved by all affected parties and be distributed and communicated to appropriate parties so that the methodology can be utilized in developing applications and managing projects. Where the SDLC methodology is not utilized in developing applications and managing projects, the justification for not adhering to the methodology should be in writing and approved.

Using a risk-based project categorization approach, EDD management should continue its current effort to enhance its SDLC methodology documents that address security requirements, including security controls and test procedures, security control reassessment, system security plan implementation, and disposal of information and media.

EDD officials stated that corrective actions to upgrade their SDLC plans to include security-related considerations in accordance with NIST guidance will not be complete until March 2009. This recommendation remains **resolved**. To close this recommendation, ETA needs to provide the OIG the policy supporting the requirement for compliance with the Software Development Life Cycle and the ITB Project Management Framework. In addition, documentary evidence showing the amended Software Development Life Cycle (SDLC), which includes the security-related sections in the Business Requirements and Architecture Description deliverables from the Solution Approach Phase.

MR #2 – Recommendation
The Assistant Secretary for ETA should ensure that EDD designate a sensitivity level for its positions and determine which positions require background screenings.

While an initiative to establish background screenings had begun after the audit the initial audit recommendation was presented to EDD officials, the initiative was derailed by local unions. The unions, in the name of preserving the privacy of its members, blocked EDD from classifying the sensitivity level between job positions and perform background screenings for current employees. EDD's has developed a ***Guide to Conducting Interviews and Reference Checks*** and follows this guide for all new employees. However, this does not meet the NIST requirement to: (1) identify position sensitivity levels so that appropriate, cost-effective screening can be completed and (2) periodically rescreen personnel in sensitive positions. Therefore the status of this recommendation remains **resolved**. To close this recommendation, EDD needs to implement a process to designate a sensitivity level for its positions, determine which positions require background screenings, and then conduct appropriate background screenings on current EDD employees.

MR #4 – Recommendations
The Assistant Secretary for ETA should ensure that EDD management:

Send notices annually to ensure that confidentiality agreements the statements are current.

The OIG tested three Tax Branch and three IT Branch (ITB) employees' confidentiality agreements and found that the branches are not consistently enforcing the policy pertaining to annual recertification of confidentiality. Our test results notes that while the three Tax Branch confidentiality agreements were current, the three ITB confidentiality agreements were over a year old. The three ITB agreements tested were beyond the annual certification requirement as they were dated, 5/29/01, 7/21/04 and 6/30/06. This recommendation remains resolved until EDD can demonstrate that its annual confidentiality policy is consistent between the branches. In order to close recommendation the OIG will have to re-test after EDD indicates it has completed corrective action.